CLAIMS

1. A transmission method comprising:

a process for a transmission system comprising an information providing server unit storing an entity file containing software for achieving an application; an administering server unit storing a security descriptive file containing authorization information showing authorization given to an application achieved when a terminal unit executes said software; and another information providing server storing an application descriptive file having contents dependent upon said entity file, into which a storage location of said entity file and a storage location of said security descriptive file are written, the process for transmitting an application descriptive file to a terminal unit when a storage location of said application descriptive file is notified by said terminal unit;

a process for said terminal unit to notify to said transmission system a storage location of said security descriptive file contained in the application descriptive file transmitted from said transmission system;

a process for said transmission system to transmit to said terminal unit said security descriptive file with security assured on the basis of the storage location of said notified security descriptive file;

a process for said terminal unit to notify to said transmission system said storage location of an entity file contained in said application descriptive file transmitted from said transmission system; and

a process for said transmission system to transmit to said terminal unit said entity file on the basis of the storage location of said notified entity file.

2. A terminal unit comprising:

a communication unit for carrying out communication with a unit in a network;

a storage unit; and

a controller,

wherein said controller comprises:

(a) means for transmitting by said communication unit to a transmission system in said network a first transmission request to receive an application descriptive file from an information providing server in said transmission system and storing the application descriptive file in said storage unit, the first transmission request containing information on a storage location of the application descriptive file, the application descriptive file containing information on a storage location of an entity file containing software for achieving an application, and information on a storage location of a security descriptive file containing authorization information showing authorization given to an application achieved by executing said software;

(b) means for transmitting by said communication unit to said transmission system a second transmission request to receive a security descriptive file, the second transmission request containing information on a storage location of the security descriptive file, contained in an application descriptive file received from said transmission system;

(c) means for transmitting by said communication unit to said transmission system a third transmission request to receive an entity file from an information providing server in said transmission system, the third transmission request containing information on a storage location of the entity file contained in an application descriptive file received from said transmission system; and

(d) means for restricting, when execution of software contained in an entity file stored in said memory unit is commanded, operation of an application achieved by execution of said software, in accordance with authorization information contained in a security descriptive file corresponding to said entity file.

3. A terminal unit of Claim 2,

wherein said transmission system assures security by transmitting to said terminal unit said security descriptive file after encrypting, and

wherein said controller comprises a means for decrypting an encrypted security descriptive file transmitted by said transmission system.

4 A terminal unit of Claim 2,

wherein said controller receives said security descriptive file by said communication unit via a communication path whose security is assured.

5. A terminal unit of Claim 2,

wherein said controller receives said security descriptive file by encrypted communication.

6. A terminal unit of claim 2,

wherein said controller receives said security descriptive file by said communication unit via a mobile communication network and an exclusive line.

7. A terminal unit of Claim 2,

wherein said controller receives said security descriptive file by encrypted communication via a mobile communication network.

8. A terminal unit of Claim 2,

wherein a means for restricting operation of an application in said controller restricts use of a resource on the basis of authorization information contained in said security descriptive file.

9. A transmission method according to Claim 8,

wherein said resource is a hardware resource inside said terminal unit.

10. A transmission method according to Claim 8,

wherein said resource is a hardware resource outside said terminal unit which said terminal unit can use.

11. A transmission method according to Claim 8,

wherein said resource is a software resource inside said terminal unit.

12. A transmission method according to Claim 8,

wherein, said resource is a software resource outside said terminal unit which said terminal unit can use.

13. A transmission method according to Claim 8,

wherein said resource is a network resource which said terminal unit can use.

14. A communication terminal of Claim 2,

wherein a means for restricting operation of an application in said controller determines a type of a use of a resource on the basis of said authorization information.

15. A terminal unit of Claim 2,

wherein said application descriptive file contains a public key of a communication provider which provides communication service to said terminal unit,

wherein said security descriptive file is signed by a secret key of said communication provider, and

wherein said controller inspects authenticity of a security descriptive file transmitted by said transmission system using a public key contained in said application descriptive file and notifies a storage location of said entity file to said transmission system only when said authenticity is proved

16. A terminal unit of Claim 2,

wherein said application descriptive file and said security descriptive file contain an application identifier assigned to a corresponding application, and

wherein said controller compares an application identifier contained in an application descriptive file transmitted by said transmission system to an application identifier contained in a security descriptive file transmitted by said transmission system, and notifies a storage location of said entity file to said transmission system only when both identifiers match.

17. A terminal unit of Claim 2,

wherein said controller notifies a storage location of said security descriptive file to said transmission system only when a storage location of said security descriptive file written in said application descriptive file is inside said administering server unit.

18. A terminal unit of Claim 2,

wherein said security descriptive file contains time limit information showing an expiration date of a corresponding application, and said controller comprises a means for repeatedly receiving said security descriptive file in a chronological order from said transmission system by repeatedly notifying a storage location of said security descriptive file to said transmission system in a chronological order; and renewing an expiration date of said application on the basis of said time limit information contained in said security descriptive file repeatedly received.

19. A terminal unit of Claim 18,

wherein said terminal unit renews an expiration date of said application only when said security descriptive file is properly transmitted from said transmission system.

20 A terminal unit of Claim 2,

wherein said terminal unit is a mobile unit.

21. A transmission system comprising:

one or a plurality of server units wherein an entity file, a security descriptive file and an application descriptive file are stored, the entity file

containing software for achieving an application, the security descriptive file containing authorization information showing authorization given to an application achieved by executing said software, and application descriptive file having contents depending upon said entity file into which storage locations of said entity file and said security descriptive file are written,

wherein a server unit among said one or a plurality of server units in which said security descriptive file is stored is an administering server unit to which authorization for administering a security descriptive file is given,

wherein each of said server units comprises a means for returning to an originator of notification a file when a storage location of said file is notified, and

wherein said administering server unit, when a storage location of said security descriptive file is notified, returns said security descriptive file to an originator of notification with security assured.

22. An administering server unit comprising:

a communication unit;

a storage unit; and

a controller which carries out,

(a) a process for writing into said storage unit a security descriptive file containing authorization information showing authorization given to an application, the application is achieved by executing software,

(b) a process for writing information on validity of said security descriptive file into said storage unit, and

(c) a process, when inquiry about validity of said security descriptive file is received by said communication unit from a terminal unit, for reading out information on validity of said security descriptive file from said storage unit, and notifying to said terminal unit the information by said communication unit.

23. A terminal unit comprising:

a communication unit;

a storage unit; and

a controller which carries out,

(a) a process for receiving from an administering server unit a security descriptive file containing authorization information showing authorization given to an application, the application is achieved by executing software, and writing said security descriptive file into said storage unit,

(b) a process for repeatedly transmitting to said administering server unit by said communication unit inquiry about validity of a security descriptive file stored in said storage unit, and

(c) a process, when a response that said security descriptive file has been voided is received from said administering server unit by said communication unit, for disabling activation of an entity file corresponding to said security descriptive file.